AMENDMENTS TO THE SPECIFICATION

Please amend the **Specification** as follows, without prejudice or disclaimer to continued examination on the merits:

On page 3, line 13 (Paragraph [0006])

[0006] ~~http://~~www.server.com/dir1/dir2/resource.htm

JB

On page 3, line ~~24~~ 18 (Paragraph [0008])

[0008] Web servers host information in the form of Web pages; collectively the server and the information hosted are referred to as a Web site. A significant number of Web pages are encoded using the Hypertext Markup Language (HTML) although other encodings using SGML, eXtensible Markup Language (XML), DHMTL or XHTML are possible. The published specifications for these languages are incorporated by reference herein; such specifications are available from the World Wide Web Consortium and its Web site (~~http://~~www.w3c.org). Web pages in these formatting languages may include links to other Web pages on the same Web site or another. As will be known to those skilled in the art, Web pages may be generated dynamically by a server by integrating a variety of elements into a formatted page prior to transmission to a Web client. Web servers, and information servers of other types, await requests for the information from Internet clients.

JB

On page 4, line ~~30~~ 27 (Paragraph [0013])

[0013] The various standards discussed herein by reference to particular RFC's are hereby incorporated by reference herein for all purposes. These RFC's are available to the public through the Internet Engineering Task Force (IETF) and can be retrieved from its Web site (~~http://~~www.ietf.org/rfc.html). The specified protocols are not intended to be limited to the specific RFC's quoted herein above but are intended to include extensions

and revisions thereto. Such extensions and/or revisions may or may not be encompassed by current and/or future RFC's.

On page 6, line 3 (Paragraph [0018])

[0018] ~~http://~~standards.ieee.org/getieee802/802.11.html; these various standards are hereby incorporated by this reference herein.

On page 6, line 22 (Paragraph [0021])

[0021] The theft of an authorized user's identity poses ~~one the~~ one of the greatest threats. Service Set Identifiers (SSIDs) that act as crude passwords and Media Access Control (MAC) addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an access point. However, existing encryption standards are not foolproof and allow knowledgeable intruders to pick up approved SSIDs and MAC addresses to connect to a WLAN as an authorized user with the ability to steal bandwidth, corrupt or download files, and wreak havoc on the entire network.

SB

On page 11, line 5 (Paragraph [0058])

[0058] In FIG. 2A, the hardware components include a single device 210A that includes a local processor serving as the system processor, or at least a portion thereof, and the one or more interfaces to the wireless network. The device 210A is preferably a mobile computer system such as a notebook computer. The local primary and/or secondary storage of device 210A may serve as the SDS; alternatively, portions of the SDS may be provided by other systems capable of communicating with the device 210A such as network addressable data storage 110, local servers 120 and/or wireless stations 170A, 170B. In some configurations, the device's interfaces to the wireless network may be limited to one or more wireless receivers. In others, the interfaces may include one or more wireless transmitters as well as one or more transmitters. If wireless transmitters are included, the

device [[~~210~~]] 210A may communicate over LAN 190 using a wireless access point 180A, 180B. In addition, included wireless transmitters may be used to support one or more of the active defense measures described in greater detail below. In some configurations, the device 210A may further include a wired connection (not shown) to Ethernet 150 allowing direct communication between it and systems connected to the wired portion of LAN 190.

On page 13, line ~~11~~ 9 (Paragraph [0062])

[0062] In FIG. 2E, the hardware components include multiple devices 220, 230A, 230B. In this configuration, the host system 220 and sensor devices 230A, 230B include the same functionality and range of components as discussed above with respect to FIGS. 2D ~~and 2E respectively~~. In such configurations, the host system 220 will typically provide a significant portion of the system processor functionality and will only have limited capacity to directly receive wireless network communication. In some of these implementations, the host system 220 may have no wireless communication interface.

On page 45, lines 6-18 (Paragraph [0179])

[0179] Various methods and functions as exhibited in various systems described above and below with respect to adaptive location tracking. In some implementations, one or more processors within architectures of the environments as described above may execute the steps in such methods and provide such functionality. The functionality may spread across multiple processing elements. In other cases, any suitable computer readable storage device, media or combination of devices and/or media, including primary storage such as RAM, ROM, cache memory, etc. or secondary storage such as magnetic media including fixed and removable disks and tapes; optical media including fixed and removable disks whether read-only or read-write; ~~paper media including punch cards and paper tape;~~ or other secondary storage as would be known to those skilled in the art, may store instruction that upon execution by one or more processors cause the one or more processors to execute the steps in such methods and to provide such functionality.

SB

On page 48, line ~~25~~ 23 (Paragraph [0198])

[0198] The information within the frame is interrogated to determine if a known attack signature has been identified in step 325. Signatures encode datalink layer attack ~~patters~~ patterns as combinations of packet sequences and state. For example, active probing emits a pattern or sequence of network requests. This sequence can be recognized by its packet sequence signature. If the attack signature is identified, the intrusion detection system signals an alarm manager to deliver an alert to the administrator in step 345.